Claims

1-5. (Cancelled)

6. (Currently Amended) A cryptographic processor, comprising:

inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field; ~~and~~

a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including a first processing unit and a second processing unit configured to determine a Montgomery product of the cryptographic parameters, the first processing unit and the second processing unit configured to receive a first bit and a second bit corresponding to the first parameter, respectively, and partial words of the second parameter; and

a field-type input in communication with the multiplication module for selection of an arithmetic operation in the multiplication module to be performed in accordance with $GF(p)$ or $GF(2^m)$ arithmetic, wherein $GF(p)$ is a prime field, $GF(2^m)$ is a binary extension field, p is a positive prime number, and m is a positive integer.

7. (Previously Presented) The processor of claim 6, wherein the first processing unit is configured to communicate intermediate values of partial words of the Montgomery product to the second processing unit.

8. (Canceled)

9. (Currently Amended) The processor of ~~claim 8~~ claim 6, wherein the arithmetic operation selectable with the field-type input is field addition.

10. (Currently Amended) The processor of ~~claim 8~~ claim 9, further comprising a dual-field adder in communication with the field-type input.

11. (Previously Presented) The processor of claim 10, wherein the first and second cryptographic parameters are represented as m bits and e words of word length w, wherein $e = \lceil (m+1)/w \rceil$, and m, e, and w are positive integers.

12-15. (Canceled)

16. (Currently Amended) A method of determining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter, the method comprising:

representing the first cryptographic parameter as a series of bits;

representing the second cryptographic parameter and a modulus as a series of words;

processing a first bit of the first parameter with each word of the modulus and each word of the second parameter to produce a first series of intermediate values and a contribution to the Montgomery product based on the first bit;

processing a second bit of the first parameter with each word of the modulus and each word of the second parameter, and a corresponding intermediate value from the first series of intermediate values to produce a second series of intermediate values and a contribution to the Montgomery product based on the second bit, wherein the first series of intermediate values and

the second series of intermediate values are determined based on a field-type input that selects an arithmetic operation to be performed in accordance with $GF(p)$ or $GF(2^m)$ arithmetic, wherein $GF(p)$ is a prime field, $GF(2^m)$ is a binary extension field, p is a positive prime number, and m is a positive integer; and

combining the first contribution and the second contribution.

17. (Canceled)

18. (Currently Amended) A computer-readable medium containing instructions for executing the method of ~~claim 17~~ claim 16.

19-21. (Canceled)

22. (Currently Amended) The cryptographic processor of claim 6, wherein the multiplication module further ~~comprise~~ comprises a third processing unit and a fourth processing unit configured to receive a third bit and a fourth bit, respectively, corresponding to the first parameter and partial words of the second parameter.

23. (New) The processor of claim 6, further comprising a dual-field adder in communication with the field-type input.

24. (New) The processor of claim 23, wherein the dual-field adder is configured to selectively execute addition corresponding to addition with carry or without carry based on the field-type input.

25. (New) The processor of claim 6, wherein the first and second cryptographic parameters are represented as m bits and e words of word length w, wherein $e = \lceil (m+1)/w \rceil$, and m, e, and w are positive integers.

26. (New) The processor of claim 7, wherein the first and second cryptographic parameters are represented as m bits and e words of word length w, wherein $e = \lceil (m+1)/w \rceil$, and m, e, and w are positive integers.

27. (New) The processor of claim 9, wherein the first and second cryptographic parameters are represented as m bits and e words of word length w, wherein $e = \lceil (m+1)/w \rceil$, and m, e, and w are positive integers.

28. (New) The method of claim 16, further comprising selecting an addition operation based on the field-type input.

29. (New) The method of claim 28, wherein the selected addition operation corresponds to addition with carry or without carry.